AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning on page 5, line 20, with the following rewritten paragraph:

--Figure 1A illustrates a system for preventing network discovery of a system services configuration according to an embodiment of the present invention. In this example, a host 102 includes an operating system 103, an application 104, and a remote authentication utility (RAU) 106. Host 102 communicates with remote addresses (as shown) ~~108-118~~ 108, 110, 112, 114, 116, and 118 via ports ~~120-130~~120, 122, 124, 126, 128, and 130. Port 120 is shown as a closed port and no data traffic passes between remote address 33.67.9.9 (118) and host 102. However, ports ~~122-130~~ 122, 124, 126, 128, and 130 are open and connection requests and probes may be sent from remote addresses ~~108-118~~ 108, 110, 112, 114, 116, and 118.—

Please replace the paragraph beginning on page 6, line 7, with the following rewritten paragraph:

--RAU 106 intercepts connection requests and probes from remote addresses ~~108-118~~ 108, 110, 112, 114, 116, and 118 to TCP ports ~~120-130~~120, 122, 124, 126, 128, and 130. RAU 106 can also be configured to intercept connection requests and probes to a pre-defined port or range of ports. Connection requests and probes can act as triggers for RAU 106, which, when received, invoke the techniques described below. Data traffic, connection requests, and probes can be composed of individual data packets. Individual (i.e., probe) or multiple data packets (i.e., bulk traffic) can be sent to host 102. A connection request can be directed by a remote address to host 102. Alternatively, a remote scanning IP address may send a number of data packets as probes to multiple hosts. To avoid exploitation of a responding host, RAU 106 tracks

connection requests and probes by their source (SRC) IP addresses, which reveal the remote address. The remote address can be used, for example, to block a specific IP address from establishing a connection over a port with host 102. In other examples, a specific IP address may be unknown to the RAU 106, which will not respond to connection requests or probes sent by the unknown IP address. In addition to preventing unknown IP address from accessing host 102, RAU 106 also enables application 104 to externally communicate with properly authenticated remote addresses.--

Please replace the paragraph beginning on page 8, line 13, with the following rewritten paragraph:

-- Figure 1B illustrates a system for preventing network discovery of a system services configuration with a RAU application according to an embodiment of the present invention. In this example, RAU 132 is similar in features and functionality to RAU 106 (FIG. 1A), but implemented as a separate application on host 102. Communicating with operating system 103 and application 104, RAU 132 intercepts connection requests to ports ~~120-130~~120, 122, 124, 126, 128, and 130 initiated by remote addresses ~~108-118~~ 108, 110, 112, 114, 116, and 118. RAU 132 intercepts connection requests and probes sent to host 102, forcing authentication of remote addresses 108-118 prior to permitting a connection to be established. Once established, the connection between host 102 and remote addresses ~~108-118~~ 108, 110, 112, 114, 116, and 118 over ports ~~120-130~~120, 122, 124, 126, 128, and 130 enables data to be exchanged between host 102, operating system 103, application 104, and any of remote addresses ~~108-118~~ 108, 110, 112, 114, 116, and 118, unless a port is closed, as shown in the case of port 120.--

Please replace the paragraph beginning on page 9, line 3, with the following rewritten paragraph:

--Figure 2 illustrates a system for preventing network discovery of a system services configuration with a RAU implemented as part of a firewall according to an embodiment of the present invention. In this example, RAU 206 is a software agent performing the functions described above, included within firewall 232. Firewall 232 may be implemented as a host or server-side application. Connection requests and probes sent to host 202 are made by remote addresses ~~208-218~~208, 210, 212, 214, 216, and 218. The connection requests and probes can be intercepted by firewall 232 in an attempt to prevent intrusions, viruses, worms, backdoors, and other unauthenticated remote addresses from gaining access to host 202. RAU 206 can hide ports ~~220-230~~ 220, 222, 224, 226, 228, and 230 by intercepting connection requests and probes at firewall 232 and preventing a response from being sent. By suppressing responses to connections requests or probes initiated by unauthenticated remote addresses, ports ~~220-230~~ 220, 222, 224, 226, 228, and 230 can be hidden from external view. Authenticated remote users may access ports ~~220-230~~ 220, 222, 224, 226, 228, and 230 if permitted by RAU 206. Access to a host via its communication ports is protected by RAU 206, as described below.—

Please replace the paragraph beginning on page 10, line 4, with the following rewritten paragraph:

--Figure 3 illustrates a process for preventing network discovery of a system services configuration according to an embodiment of the present invention. In this example, a specific port to be opened is identified (302). The identified port is then opened (304). Based on data traffic received at the open port, RAU 106 can intercept connection requests, probes, and other data packets sent by remote addresses (i.e., remote addresses ~~108-118~~ 108, 110, 112, 114, 116, and 118) at the open port (306). As discussed herein, connection requests, probes, and scans are composed of one or more data packets. In general, any data traffic sent to a port can be composed of one or more data packets. Connection requests and probes may be handled by

RAU 106 and can require authentication of the remote address requesting a connection. Upon receipt RAU 106 attempts to authenticate the packet(s) (308). If the packet is authenticated, in this example, then a port with a network service operating on it is opened for a configurable time period (310). The configurable time period is a window during which an authenticated remote client (for example, clients ~~118-116~~118, 116) may establish a connection with the host 102 (312). Once a connection is established the port can be closed to prevent any further remote use or exploitation. Also in this example, if a packet or other incoming data traffic fails to properly authenticate, then the port may also be closed or kept closed in order to prevent remote access or exploitation (314).--

Please replace the paragraph beginning on page 11, line 1, with the following rewritten paragraph:

-- Figure 4A illustrates a process for protecting a host against remote port scanning and discovery of a system services configuration according to an embodiment of the present invention. RAU 106 is passively monitoring or "listening" to ports ~~120-130~~120, 122, 124, 126, 128, and 130 to determine if a connection request or probe is received (402). If, for example, port 120, is not protected by RAU 106, then port 120 is placed into a stealth mode to prevent any response being sent back to the remote address (404). If RAU 106 determines that an access attempt in the form of a connection request or probe was sent to port 120, then it also determines if port 120 is designated as a RAU-protected port (406). If a port is protected or not published as a known port for external access, then RAU 106 determines if the requesting remote address 118 is allowed access (authenticated) (408). If the remote address is authenticated, then the targeted port may be opened to enable access and a connection to be established. Published ports, in this context, refers to ports that are known to a host and associated with a particular set of characteristics (i.e., authorized for access). Published ports can be made available to a remote

address for connecting to a network service on the system 100, provided proper authentication occurs.—

Please replace the paragraph beginning on page 13, line 10, with the following rewritten paragraph:

-- RAU 106 prevents unauthenticated remote addresses from scanning ports ~~120-130~~120, 122, 124, 126, 128, and 130, for example, and exploiting vulnerabilities based on information or data gathered in response to a failed connection request or probe. RAU 106 can also prevent unauthenticated access by passively monitoring incoming data traffic. Upon properly authenticating a remote address, RAU 106 may direct operating system 103 to open a port for a configurable period of time in which to establish an authenticated connection.—

Please replace the paragraph beginning on page 14, line 19, with the following rewritten paragraph:

-- Figure 6 illustrates an architectural schema of an exemplary remote authentication utility (RAU) 634 that prevents network discovery of a system services configuration according to an embodiment of the present invention. In this example, hosts 602 and 618 are illustrated in terms of protocol stacks in accordance with system architectural schemas such as the Open Systems Interconnection (OSI) model. Several layers are shown for each of hosts 602 and 618. Application 604, 620, Presentation 606, 622, Session 608, 624, Transport 610, 626, Network 612, 628, Data Link 614, 630, and Physical 616, 632 layers are shown. RAU 634, which is similar to RAU 106, 132, and [[203]] 206 functions at the network layer or "stack" level of the architectural schema. At the network stack, RAU 634 is a component ensuring authenticated flow of data traffic between hosts 602 and 618. RAU 634 can provide routing and authentication features such as those described above which permits an authenticated connection to be initiated and established between hosts 602 and 618. By interfacing with the network stack, RAU 634

intercepts the individual data packets that comprise connection requests, probes, or any other data traffic sent to a host it protects. However, RAU 634 can also integrate at other layers, multiple layers, or in other architectural schemas (e.g., SNA, DNA, etc.).

--